THE RIGHT TO PRIVACY AND CONFIDENTIALITY

SILVIA VITRO'
1/6/2022

1) CONFIDENTIAL INFORMATION AND PERSONAL DATA

1.1) Confidential Information

a) What **confidential information** needs to be protected in industrial property court proceedings?

List:

-**trade secrets**, subject to recent Community and national regulations;

-**technical and commercial information** relevant to the entrepreneur, even if not of such a nature and value as to constitute Trade Secrets proper;

-**technical data** covered by the various industrial property titles (patents, models);

-**company and personal data** that may be found on personal computers subject to inspections and descriptions.

b) Analysing more specifically
the category of **Trade secrets**,
it is noted that, initially,
in Italian law, they were protected
through the rules of the civil code repressing acts
of **unfair competition**.

The Italian legislator then introduced *a first specific discipline* in 1996, prompted by the TRIPs Agreement (article 6 bis of the Inventions Act, which explicitly qualified the abusive exploitation of secret information as *unfair competition* behaviour, which meant that protection could only be invoked against certain parties, such as the competitors of the owner of the information).

With the introduction of the **Italian Industrial Property Code** in 2005, *Art. 6 bis of the Invention Law* was repealed and its contents were recast in Art. 98 and 99 of the IPC, with the consequent application of the procedural rules and means of protection provided by the IPC for other industrial property rights.

The **EU Directive 2016/943**, ***Trade Secrets***, of the European Parliament and of the Council, 8/6/2016, on the protection of *know-how* and *commercial information* against unlawful acquisition, use and disclosure, was then issued; it **strengthens the protection** of secrecy, defining the asset to be protected and identifying effective protection measures, and at the same time is aimed at **harmonising** the provisions on the subject within European legislations.

In Italy, the Directive has been transposed through Legislative Decree 11/5/2018 no. 63.

Directive 2016/943 provides for a **minimum degree of harmonisation** (Art. 1: "*Member States may, in compliance with the provisions of the TFEU, provide for more farreaching protection against the unlawful acquisition, use or disclosure of trade secrets*").

Some of the jurisdictional measures referred to in Directive 2916/943 had already been introduced into our legal system when the so-called *Enforcement Directive* (2004/48/EC, implemented by Legislative Decree No. 140/2006) was transposed.

The **mechanism for protecting** *trade secrets* is **different** from the other type of industrial property that is the patent.

The exercise of an exclusive right can be based first and foremost on maintaining secrecy. This implies that the entrepreneur provides himself with all appropriate means to conceal his invention from competitors, through de facto measures (requiring appropriate investments in security) and through legal instruments (confidentiality pacts, trust deposits, escrow agreements - which can be concluded between entrepreneurs and employees).

The alternative for the rightful owner of a secret to secure exclusivity is patent protection, subject to registration, if the information meets legal requirements. At the same time in these cases, the community must tolerate a monopoly situation for the duration of the patent.

The European Observatory on Infringements of Intellectual Property Rights (EUIPO), in a study published in July 2017, analysed, from a legal and economic perspective, trade secrets used by European companies, realising that companies (especially small and medium-sized enterprises, SMEs) **use trade secrets more frequently than patents**, especially in the areas of *innovative* production *processes* and *services* (while patents are more often used for *novelties concerning tangible goods*).

The advantages of *trade secret* protection include:
- the duration of protection, which is not limited to a fixed term;
- the breadth of the object of protection: it can include new manufacturing processes, improved recipes, information on customers and suppliers, in short, even anything that does not qualify for patenting;
-information protected through a trade secret may play a strategic role for the company, either for decades (think of the formula of a chemical compound, the famous Coca Cola recipe) or for a much shorter period (as in the case of the results of a *marketing* study, based on the name, price and launch date of a new product or the price offered in a tender procedure);
-the absence of the need for formal recognition, with no related costs;
-the possibility of applying the secrecy regime to the innovation early in the creative process, without requiring a description of the invention.

The disadvantages of trade secrets compared to titled industrial property rights are:
-at the evidentiary level before the courts (patents, registered trademarks, designs grant innovators a certain, though often time-limited, exclusive right);
-the need for substantial investment and ongoing expenditure for internal controls and to protect secrets from misappropriation.

The EUIPO study found that companies' use of Trade Secrets is higher than patents in the following sectors (which are more rapidly obsolete and therefore not worth patenting): electronic technologies and products, film and television operators, software, financial services, insurance companies and pension funds, and architectural and engineering services.

According to the above-mentioned report, there is limited use of trade secrets and patents to protect innovations **in Italy**.
In fact, informal protection tools are often used, such as
lead time advantages (i.e. the practice of commercialising innovation as quickly as possible in order to benefit from *first mover advantages*)
or *complexity of goods/services* (i.e. the complex design of a product in order to prevent even partial copying of the design by a competitor - a practice known as *reverse engineering*).

Pursuant to **Art. 98 of the CPI** (as reformed by the aforementioned Directive)
Trade secrets *means* ***business information*** *and* ***technical-industrial experience****, also the* ***commercial ones****, subject to the legitimate control of the holder, whether such information:*
a) *is* ***confidential****, in the sense that* ***as a whole*** *or in* ***its precise configuration and combination*** *of its elements it is not* ***generally known*** *or* ***easily accessible*** *for experts and operators in the field*;
b) *has an* ***economic value*** *as much as it is confidential*;
c) ***is subject****, by the persons to whose legitimate control it is subject,*
to measures to be considered reasonably adequate *to keep it confidential*

The two relevant types of secrecy emerge from the aforementioned rule:

-**technical secrets**: confidential information relating to a product or an industrial process, whether patentable or not ('technical know-how').

-**commercial secrets**: confidential information concerning the company's commercial organisation (such as 'customer lists', data linked to so-called 'customer profiling' via the Internet, orders history linked to each customer).

Pursuant to **Art. 99** IPC (as reformed):

1. *Without prejudice to the provisions on unfair competition,* ***the legitimate holder*** *of the trade secrets as per article 98,* ***has the right to prohibit*** *third parties* (so even non-competitors)*, subject to his consent,* ***from acquiring, disclosing*** *to third parties or* ***using*** *that information and experience* ***in an abusive manner****, except for cases in which the third party has obtained it in an independent manner by the third party*

It is noted, inter alia:

-that **non-abusive acquisition** is for example *'reverse engineering'*;

- that **non-abusive disclosure** is for example that of the newspaper revealing a chemical formulation harmful to health;

-that **non-abusive use** can be use of a secret technology for private domestic use

1-bis. *The acquiring, using or disclosing of* ***trade secrets*** *as per article 98 are considered illegal* ***even when*** *at the moment of the acquiring, utilization or disclosing,* ***the subject was aware*** *of, or according to the circumstances,* ***should have been aware*** *of the fact that the trade secrets had been obtained directly or indirectly* ***by a third party*** *which* ***used then or disclosed them illegal****, as per paragraph 1*

1-ter. *The **production**, **offer**, **commercialization** of **products which constitute a violation**, or the importation exportation or storage of the same products, **constitute an unlawful use** of trade secrets of article 98, if the subject who realized those behaviours **was aware of** or, according to the circumstances, **should have been aware** of the fact that the trade secrets had been used unlawfully as per paragraph 1.*

***Products which constitute a violation** mean the products of which **designs**, **characteristics in an important manner**, **function**, **production** or **commercialization** take benefit from the abovementioned trade secrets acquired, used or illegally disclosed*

-**Products which constitute a violation** can mean not only those made **by exploiting a technical secret**, but also those made by exploiting a commercial secret

(e.g. goods made with characteristics particularly liked by a specific list of purchasers, unlawfully taken away from the holder, or goods sold only in a certain territory, where it has been found that the clientele inclined to purchase them is greater).

1.2) Personal Data

Regulation (EU) 2016/679 (GDPR - *General Data Protection Regulation*) regulates **the processing of personal data** in the European Union;
this regulation has been applicable in all member states since 25 May 2018.

With this regulation, the European Commission aims **to strengthen the protection of personal data** of EU citizens and residents, both within and outside the EU borders, by giving citizens back control of their personal data, unifying and homogenising privacy laws within the EU.

Since its entry into force, the GDPR has **replaced** the contents of the *Data Protection Directive* (Directive 95/46/EC) and, in Italy, has **repealed** the articles of the *code for the protection of personal data* (Legislative Decree no. 196/2003) that are incompatible with it.

The GDPR reinforces the role of information as an instrument of transparency and the **centrality of the data subject's consent** to the processing of their data.

Processing is only permitted for specific and declared purposes, to the extent necessary.

The right to obtain the deletion of one's personal data (the so-called *'right to be forgotten'*) is also provided for.

The data subject's consent to the processing of personal data must be free, specific, informed and unambiguous, even if expressed by electronic means or with a simple flag.

Personal data (ex art. 4 GDPR): is **information** that **identifies or makes identifiable**, directly or indirectly, **a natural person** and that can **provide information** on his or her characteristics, habits, lifestyle, personal relationships, health status, economic situation, etc.

Particularly important are **data that allow direct identification** - such as personal data (e.g. first name and surname), images, etc. - and **data allowing indirect identification**, such as an identification number (e.g. tax code, IP address, number plate).

Moreover, with the evolution of new technologies, **other personal data** have taken on a significant role, such as *those relating to electronic communications* (via the internet or telephone) and *those allowing geolocalisation*, providing information *on places frequented and movements*.

In a question, the European Commission replied that 'even **various pieces of information which, collected together**, can lead to the identification of a given person constitute personal data': this is the concept of a **profile** (of behaviour, habits, history) which becomes personal data even though it does not contain, in itself, a specific piece of information identifying a given subject.

The **'special categories of data'** under **Art. 9 GDPR** (traditionally considered **'sensitive data'**) refer to **personal data revealing** racial or ethnic origins, political opinions, religious beliefs, philosophical convictions or trade union membership, as well as genetic data and biometric data, or data relating to a person's health and sex life.

Turning to the **definition of processing**, it should be noted that it is a broad and inclusive notion since it contemplates *even complex conducts*, aimed not only at *the collection and storage of data* (or at their communication), but also conducts such as *the processing, modification, selection, extraction, comparison, use, interconnection, blocking, communication, dissemination, deletion and destruction of data*, even if not registered in a database.

With the emergence of ***Big Data***, the notion of 'personal data' also **expands**, and thus the need for the relevant processing *to take place in a privacy-friendly manner*.

Measures to ensure the security of personal data are presented in **Art. 32**:

(a) the **pseudonymisation** and encryption of personal data (which in general can also be achieved by *data masking*);
(b) **the ability to ensure** the confidentiality, integrity, availability and resilience of processing systems and services *on a permanent basis*;
(c) **the ability to restore timely** availability and access to personal data in the event of a physical or technical incident;
(d) **a procedure** for regularly testing, verifying and evaluating the effectiveness of technical and organisational measures to ensure security of processing.

The controller and data processor bear the *burden* of demonstrating that their systems comply with the European regulation. They may adhere to *codes of conduct*, or to *certification of compliance*. *Certification does not reduce the responsibility of the controller or the processor*, nor the powers and tasks of the authorities (Art. 42(4)), and has a maximum duration of five years (Art. 43(4)).

A personal data breach is defined as a security breach that *accidentally or unlawfully results* in the *distribution, loss, modification, unauthorised disclosure of or access* to personal data transmitted, stored or otherwise processed.

It can be a *malicious event* such as a *cyber attack* but also accidental such as a natural disaster or the simple loss of a USB stick.

The right to portability is enshrined in Article 20: *"**The data subject** shall have the right to receive the **personal data** concerning him or her, which he or she **has provided to a controller**, in a structured, commonly used and machine-readable format and have **the right to transmit those data to another controller** without hindrance from the controller to which the personal data have been provided"*

An individual must therefore be able to transfer his or her personal data from one electronic processing system to another without hindrance.

The aim of this right is **to facilitate the transfer and exchange of data** by avoiding **technological lock-in phenomena** and promoting **the free flow of data** by stimulating **competition** between data controllers.

1.3) **'Privacy' and 'Confidentiality'** (or 'confidentiality'), therefore, are **two clearly distinct concepts** framed by different doctrines and laws.

Invoking privacy rules to protect *secret information or confidential business and professional data* is totally unfounded**.**

2) THE PROCEDURAL PROTECTION OF CONFIDENTIAL INFORMATION

2.1) The rules of the Industrial Property Code on trade secrets

-Art. 121-*ter* CPI
«***Protection of the confidentiality***
of trade secrets ***during the judicial proceedings***»:

1. ***In the proceedings*** *related to the unlawful acquiring, using or disclosing of* ***trade secrets*** *referred to article 98****, the judge can prohibit*** *the* ***use or the disclose of the trade secrets*** *involved in the proceedings, he assumes to be confidential,* ***to the persons*** *indicated or authorized by him, to the parties and their representatives and consultants, to the lawyers to the administrative personnel, to the witnesses and* ***to the other subjects which could have access*** *to the decisions, acts and documents contained in the file of the Judicial Authority.*

The prohibition order under sentence1 is declared ***as a consequence of request of a party*** *and* ***remains in force*** *also* ***after*** *the conclusion of the proceedings during which it was adopted.*

In the absence of any indication by the legislator as to the timing and modalities for filing the application, it seems possible to file it **at any stage and level of the proceedings**, with an effectiveness not unlike that of a precautionary measure in the course of proceedings.

The order imposing confidentiality **remains effective even after** the conclusion of the proceedings.

The provision is intended to maintain confidentiality **not only as to the information that the plaintiff or the claimant will ask** the court to protect, **but also as to information that the defendant** may deem appropriate to produce for its own protection and which in turn deserves to be kept secret.

-Art. 121-*ter* CPI

2. *The order under paragraph 1* ***loses its effectiveness****;*

a)if ***with a final decision*** *is confirmed that the trade secrets involved in the proceedings did not fullfill the requirements under article 98;*
b)if the trade secrets ***become generally known or easily accessible*** *by the experts and the operators in the relevant field*

-Art. 121-*ter* CPI

3. ***In the judicial proceedings*** *referred to in paragraph 1,* ***under the request of a party****, the judge* ***can adopt the measures*** *which, according to the principles of the due process,* ***seems to be more adequate*** *to protect the confidentiality of* ***the trade secrets involved in the proceedings*** *and in particular:*

*a)****to limit*** *to* ***a restricted number*** *of subjects* ***the access*** *to the hearings and to the acts and documents included in the file of the judicial Authority*

b)to dispose, ***in the decisions defining*** *the proceedings under paragraph 1, which are made available also to subjects other than the parties,* ***the obscuration or the omission*** *of the parts containing the trade secrets*

EU Directive 2016/943, in **Article 9**, II, specified: "***The number of persons****…shall be* ***no greater than necessary*** *in order to ensure compliance with the right of the parties to the legal proceedings* ***to an effective remedy*** *and to* ***a fair trial****, and shall include, at least,* ***one natural person*** *from each party and* ***the respective lawyers*** *or* ***other representatives*** *of those parties to the legal proceedings*".

Directive 296/943 provided, in Article 9(1), that the judge could also take the above measures **on his own initiative**.

Italy opted **to exclude this possibility** of acting ex officio, leaving it up to the persons concerned to decide whether or not to request protection, considering **also the high degree of technicality** required to assess the need for procedural measures to protect confidentiality.

A connection can be discerned between **Art. 121 ter 3b** - obscuration of data in the judgment - and **Art. 126**(1) - choice of method of publication of the order permitting protection of trade secrets.

-Art. 121-*ter* CPI

4. ***To the purposes under letter b), paragraph 3****, the judge, with the decision,* ***indicates the parts*** *that the clerk has* ***to redact or to omit*** *when gives a copy of the decision to subjects other than the parties.*

For the same purpose *the judge orders that, when the decision is published* ***the clerk has to add a note*** *from which it results* ***the prohibition*** *for the parties to publish the decision in the complete version*

This is always a measure **for the protection of the confidentiality** of *trade secrets* (*'For the purposes of paragraph 3(b)'*), **not** for the protection of **personal data**.

-Art. 126 CPI «***Publication*** *of the judgment*»

1. The judicial authority may order that **the interim relief order** or **the judgment** that **determines the infringement** of the industrial property rights **be published** in full or as a summary, or only the ruling of the judgment, taking into account the seriousness of the circumstances in one or more newspapers indicated by it, at the expense of the losing party. **In any case**, the **adequate measures for the protection of the confidentiality** of the **trade secrets** referred to in the article 98 **are adopted**

For instance, by the **obscuration or the omission** of the parts containing the trade secrets (art. 121)

2.2) The rules of the Industrial Property Code on patents

-Art. 67 CPI (“*Patent of a process*”)

1. *In the case of a **patent of process**,*

*each product identical to that obtained through the patented process **is presumed to be obtained** by way of that process, unless demonstrated otherwise, if either:*

*a) the **product** obtained through the process is **new**, or*

*b) there is a **substantal probability** that the identical product has been manufactured through the process and if the owner of the patent **has not succeeded**, through a reasonable effort, in determining the process actually carried out;*

2. ***In order to provide contrary evidence**, the **legitimate interest of the party** accused of infringement **to the protection of his manufacturing and business secrets** must be taken into account*

2.3) The rules of the Industrial Property Code in general

- Art. 121 CPI (*Allocation of the burden of proof*):

1. *Except for the case of revocation for non-use,* ***the burden of proving*** *the nullity or forfeiture of the title of industrial property always* ***lies with the party*** *that challenges the title. Subject to the provision of article 67,* ***the burden of proving*** *infringement* ***lies with the owner****. In every case in which is claimed or objected the revocation for non-use, the owner gives evidence of the use of the trademarks pursuant to article 24.*

2. ***If a party has provided serious evidence*** *that its claims* ***are grounded*** *and* ***has identified*** *documents, elements or information held by the other party that confirm such evidences,* ***it may request that the Court orders their exhibition*** *or* ***request the information*** *from the other party. The party may also request that the Court* ***orders the other party to provide the elements*** *for the identification of the* ***persons involved*** *in the production and distribution of the goods or services that consitute an infringement of the industrial property right.*

2-bis. ***In the event*** *of an infringement committed* ***on a commercial scale through acts of piracy*** *as per article 144,* ***the judge****, on request from the party, may also order* ***the exhibition of the banking, financial and commercial documentation*** *that is in the possession of the other party.*

3. *In taking the measures identified above,* ***the judge*** *shall* ***adopt measures suitable to guarantee the safeguarding*** *of* ***confidential information****, after consulting with the other party*

In the event that **the plaintiff's application for evidence** is admitted and **documents in the other party's possession are exhibited** or **information is requested** from it, the court must take **appropriate measures to ensure the protection of confidential information**.

For instance, it may be ordered that **all data**

in the documentation that is

not strictly related

to the subject matter of the proceedings **be blacked out**.

Or it may be ordered that **part of the exhibited documentation** be **examined only by certain persons**, such as the court expert (technical or accounting).

- **Art. 129 CPI** (*Description and seizure*):

1. *The owner of an industrial property right* ***may request the description or seizure*** *and also the seizure conditional on the description,* ***of some or all of the items*** *constituting an infringement of that right, as well as* ***the means*** *used for their production and of the* ***elements of*** *concerning the reported infringement and its entity* ***The measures necessary*** *to* ***guarantee the safeguarding of confidential information*** *shall* ***be adopted****.*

- **Art. 130 CPI** (*Execution of description and seizure*):

1. ***Description and seizure*** *are* ***carried out*** *by the* ***bailiff****, with the assistance of one or more* ***experts****, where necessary, and also with the use of* ***technical means*** *of inspection, photographic or other equipment.*

2. ***The interested parties*** *may be authorized* ***to be present*** *during the operations, including* ***by way of their representative****, and to be assisted by* ***technicians*** *chosen by them.*

The protection of confidential information is granted on a broad spectrum and concerns **the entire subject** matter of the measure and of the evidentiary acquisition (both the *objects* constituting infringement of the right, the *means* used to produce them, and *the evidence* concerning the alleged infringement and its extent).

The power to adopt the measures **lies with the judge**, who may, however, **limit himself to indicating** in a general way the **guiding criteria** and the **operating methods**, entrusting their concrete and specific application **to the judicial officer** and **to the technical auxiliary** assisting him, endowed with the necessary professional competence.

In the execution of the precautionary measures of **description** and **seizure**, according to **judicial practice**, **three levels of protection** of confidential information are followed:

1) **Unlike** in the UPC and ROP rules, applicants for the measures **may be present** at the execution of description and seizure;
-may also not attend in person, but **through their representatives and technicians**;
-**however**, for the purpose of protecting confidential information, including that of the defendant, the judge may **limit access** to the *documentation* or examination of the data *on the personal computers* only **to certain persons**, such as the *bailiff*, the *court-appointed technical expert* and the *party's technical consultants*, all of whom are **bound to professional secrecy**, also with respect to the parties to the proceedings (plaintiff and defendant);
-also, **security** deposit may be imposed on the claimant (pursuant to Article 669 undecies of the Code of Civil Procedure);

2) A second level of caution **places responsibility** on the prosecuting judicial **bailiff** and the **technical assistant**, who, following the recommendations and general criteria given by the judge in the order, **must select** only the *relevant information*, **eliminating** all information, whether technical or commercial, *that is irrelevant* to the subject of the investigation concerning the alleged infringement of an industrial property right;

3) The third level concerns the **secrecy of the documents** (paper or hard disk) taken, through the **custody in closed envelopes**, suitably sealed and sent to the court registry;

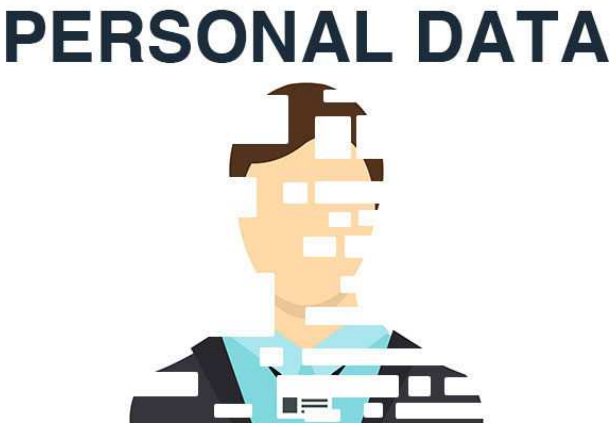
-this practice postpones **to a more appropriate venue** (the hearing) the **adversarial discussion** of what is to be acquired and what is to be expunged, following the **de-secretion** of the evidentiary material.

The applicant and other interveners are obliged:

-**to maintain secrecy** **even if** the precautionary measures are **subsequently modified or revoked**

-and in any case **not to use** and disseminate **data** on competitors and third parties, acquired in the course of the aforementioned description and seizure proceedings, otherwise unfair competition will be committed.

3) THE PROTECTION OF PERSONAL DATA IN THE IP PROCESS



a) IP Process

-Art. 126 CPI (*Publication of the judgement*):
Protection of the **'natural person**'
in the event of publication of the order or judgment.
1-ter. *For the purpose of the paragraph 1-bis,*
the judge considers also ***if the information about the author of the violation*** *allow the* ***identification of a natural person*** *and, in this case, if the publication of such information is* ***justified****, also considering the possible damages which the measure could cause in the* ***private life*** *and to the* ***reputation*** *of the same author*

This **does not concern the protection of trade secrets**, as in the previous paragraphs, but **the protection of the individual**.

No such protection is expressly provided for **other cases of infringement** of industrial property rights (e.g. designs, patents, or trade marks).

b) The obligation to anonymise court **decisions** (except in specific cases, such as child protection) **is not provided for** in **Regulation (EU) 2016/679** of the European Parliament and of the Council of 27 April 2016, *'on the protection of individuals with regard to the processing of personal data*' (which became fully applicable as of 25 May 2018).

The exclusion of the Supervisor's **control** over **the civil judicial authority** emerges, for instance:

- from **Article 9**(2)(f) ("*1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. 2. Paragraph 1 shall not apply if one of the following applies: f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity*);

-from **Article 17**(3)(e) and **Article 18**(2): ("*1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed….3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: e) for the establishment, exercise or defence of legal claims*").

b) <u>Privacy Code</u>

Privacy Code
(Legislative Decree No. 196 of 30/6/2003, as amended), provides:

Chapter III – Legal Information

-**<u>Art. 51</u>**: *General Principles*

1. Without prejudice to the provisions of the procedural provisions concerning the inspection and issue of excerpts and copies of acts and documents, ***the data identifying matters pending before a judicial authority*** *of any order and level* ***shall be made accessible*** *to any interested party also by means of electronic communication networks, including the institutional site of the same authority on the Internet.*

2. ***Judgments and other decisions*** *of the judicial authority of any level and grade filed in the registry or secretariat* ***shall also be made accessible*** *through the information system and the institutional site of the same authority in the Internet network,* ***observing the safeguards*** *provided for in this Chapter.*

-**Art. 52**: *Data identifying the interested parties*

1. Without prejudice to the provisions concerning the wording and content of judgments and other measures of judicial authority of any order and degree, **the interested party may request**, for **legitimate reasons**, by filing a request at the registry or secretary's office of the proceeding office before the conclusion of the relevant court proceedings, **that an annotation** be made **by the same registry** or secretary's office, **on the original of the judgment or order**, in order **to preclude**, in the event of reproduction of the judgment or order in any form whatsoever, **the indication of the personal particulars and other identifying data** of the same party appearing on the judgment or order.

2. On the request referred to in paragraph 1 the authority that pronounces the judgement or adopts the measure **shall decide** by decree, without further formalities. **The same authority may, ex officio**, **order** that the annotation referred to in paragraph 1 be made **to protect the rights or dignity of the persons concerned**.

3. In the cases referred to in paragraphs 1 and 2, when the judgment or order is filed, **the clerk of the court** or secretary's office **shall make and sign** thereon, also with a stamp, **the following annotation**, indicating the particulars of this Article: **'In case of disclosure omit personal details and other identifying information of**.....".

4. **In the event of dissemination also by third parties** of judgments or other measures **bearing the annotation** referred to in paragraph 2, or of the relevant legal holdings, the personal particulars and other identifying data of the person concerned **shall be omitted**.

5. Without prejudice to the provisions of Article 734-bis of the Penal Code concerning persons offended by acts of sexual violence, **any person who circulates judgments or other judicial decisions** of any order and degree **shall in any event**, even **in the absence of the annotation** referred to in paragraph 2, **omit personal details**, other identifying data or other data also relating to third parties, **from which the identity of minors** or of the parties in proceedings concerning **family relations** and the **status of persons** may be inferred even indirectly.

6. The provisions of this article **shall also apply when an award is filed** pursuant to Article 825 of the Code of Civil Procedure. The party may make the request referred to in para. 1 to the **arbitrators** before the award is rendered and the arbitrators shall make the annotation referred to in para. 3 to the award, also in accordance with para. 2. The arbitration panel established at the Arbitration Chamber for Public Works pursuant to Article 209 of the Public Contracts Code referred to in Legislative Decree No. 50 of 18 April 2016 shall do likewise in the event of a request by a party.

7. **Outside the cases indicated in this Article**, the dissemination **in any form of the content**, including in full, of judgments and other judicial orders **shall be permitted**

In conclusion, Articles 51 and 52, **allow the full dissemination**, also by means of the network or computer media, **of judicial decisions** of all orders and degrees**, except in cases where anonymisation has been ordered** or **data must be obscured by law**.

The sentence **at the end of the judgment** is as follows:

- "***Pursuant to the Privacy Code****, it is ordered that in the event of dissemination of this order,* ***the names and other identifying data*** *of the parties and any other third parties mentioned in the order* ***be omitted***."

I conclude by observing that **a complete anonymisation of judicial decisions** makes them **hardly comprehensible** and hardly usable as precedents.

In fact, **the construction of a database** of **judicial precedents** (also for the purpose of the exercise of so-called *predictive justice*) necessarily implies the filing of maxims correlated **by even brief descriptions of the fact**, so that the precedent may be comprehensible.

Which would not be possible, **especially in the field of industrial law**, in the case **of total anonymisation of measures** (think of the case where in a *trade mark comparison* judgement these are only represented by asterisks).

Goodbye